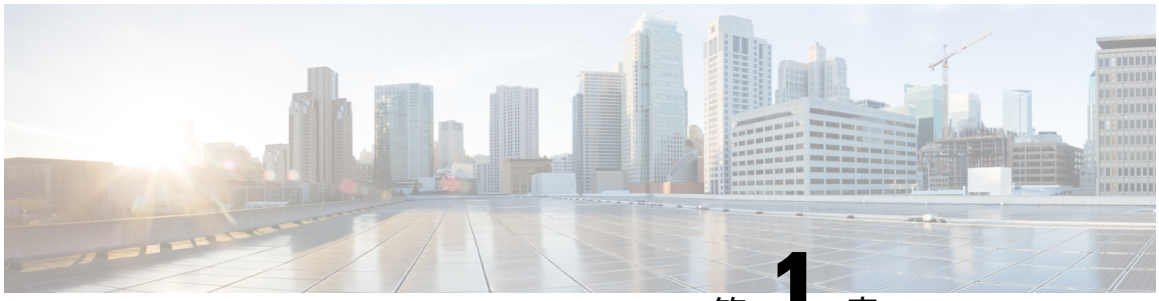
シスコセキュリティ分析とロギング（オンプレミス）スタートアップガイド v2.0 および 3.0

初版：2021 年 5 月 26 日

最終更新：2022 年 4 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



第 1 章

シスコのセキュリティ分析とロギング（オンプレミス）スタートアップガイド：ファイアウォールイベントの統合

（注） オンプレミスではなく Cisco Cloud にファイアウォール イベント データを保存する場合、詳細については Cisco Security Analytics and Logging（SaaS）のマニュアルを参照してください。

概念とアーキテクチャ

セキュリティ分析とロギング（オンプレミス） の展開では、Secure Network Analytics アプライアンスを使用して別のシスコ製品の展開環境（Firepowerアプライアンス展開など）からのデータを保存します。Firepower 展開の場合、Firepower セキュリティイベントおよびデータプレーンイベントをFirepower Management Center が管理する Firepower Threat Defense デバイスから マネージャ にエクスポートして、その情報を保存します。セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0 では、syslog を介して ASA デバイスから マネージャ にイベントをエクスポートする機能が追加されました。

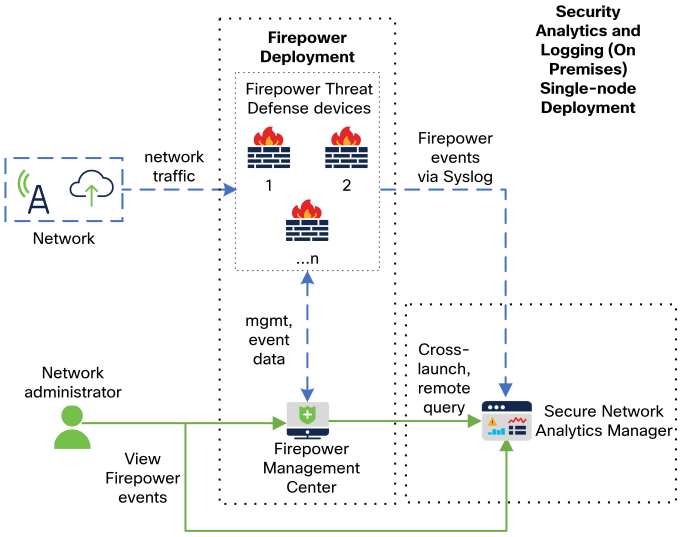
Secure Network Analytics の展開には次の 2 つのオプションがあります。

- 単一ノード：スタンドアロンのManagerを展開してイベントを受信および保存し、そこからイベントを確認および照会します。

- マルチノード：イベントを受信する Cisco Secure Network Analytics フローコレクタ、イベントを保存する Cisco Secure Network Analytics データストア（Cisco Secure Network Analytics データノード X 3 を装備）、イベントを確認および照会できる Manager を展開します。

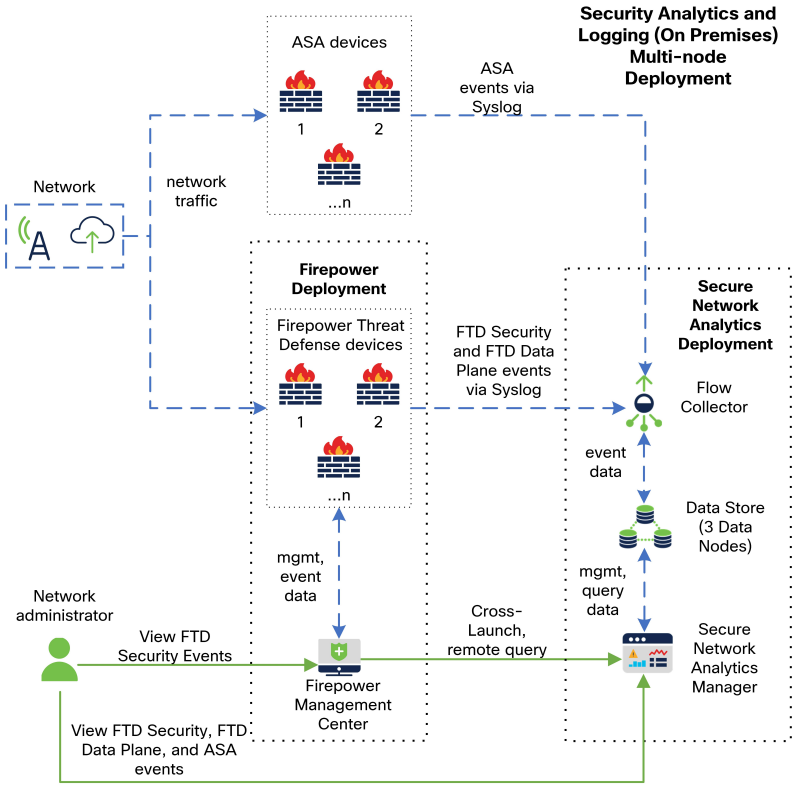
（注） スタンドアロンのアプライアンス（単一ノード）としての マネージャ のインストール、またはフローコレクタと3つのデータノード（マルチノード）を管理するマネージャのインストールがサポートされています。3 つのデータノードを管理せずに 1 つ以上のフローコレクタを管理する場合は、マネージャにアプリケーションをインストールすることはできません。詳細については、トラブルシューティングを参照してください。

マネージャ を使用した 単一ノード の展開の例については、次の図を参照してください。



この展開では、Firepower Threat Defense デバイスは Firepower のイベントを マネージャ に送信し、Manager がこれらのイベントを保存します。ユーザは Firepower Management Center の UI からマネージャ を相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。

マネージャ、3つのデータノード、およびフローコレクタを使用したマルチノードの展開の例については、次の図を参照してください。



この展開では、Firepower Threat Defense デバイスおよび ASA デバイスはファイアウォールのイベントをフローコレクタに送信します。フローコレクタは、保存のためにデータストア（データノード X 3）にイベントを送信します。ユーザは Firepower Management Center の UI から マネージャを相互起動して保存されたイベントに関する詳細情報を表示できます。また、Firepower Management Center からリモートでイベントを照会することもできます。

参考資料

次の表に、セキュリティ分析とロギング（オンプレミス）アプライアンスの互換性、展開、使用に関する参照資料を示します。

表 *1*：

ドキュメント	説明
Firepower Release Notes	『Firepower Release Notes』を参照して、最新の Firepower リリースに関する最新情報（直前の情報を含む）を確認してください。

ドキュメント	説明
Secure Network Analytics Smart Licensing Guide	Secure Network Analytics の製品インスタンスを登録し、Secure Network Analytics アプライアンスのライセンスを取得する方法については、『Secure Network Analytics Smart Licensing Guide』を参照してください。
Secure Network Analytics Installation Guide	単一ノード展開の場合に Secure Network Analytics アプライアンスを展開する方法については、『Secure Network Analytics Installation Guide』を参照してください。
Secure Network Analytics Configuration Guide	単一ノード展開の場合に Secure Network Analytics アプライアンスを設定する方法については、『Secure Network Analytics Configuration Guide』を参照してください。
Secure Network Analytics Data Store Deployment and Configuration Guide	マルチノード展開の場合に Secure Network Analytics アプライアンスを設定する方法については、『Secure Network Analytics Data Store Deployment and Configuration Guide』を参照してください。
Secure Network Analytics Release Notes	『Secure Network Analytics Release Notes』を参照して、最新の Secure Network Analytics リリースに関する最新情報（直前の情報を含む）を確認してください。
セキュリティ分析とロギング（オンプレミス）Release Notes	『セキュリティ分析とロギング（オンプレミス）Release Notes』を参照して、最新のセキュリティ分析とロギング（オンプレミス）リリースおよびセキュリティ分析とロギング（オンプレミス）アプリケーションに関する最新情報（直前の情報を含む）を確認してください。

Firepowerをまだ展開していないか、または予想される接続、侵入、ファイル、およびマルウェアのイベントを生成するように Firepower 展開を設定していない場合は、次を参照してください。

表 *2:*

ドキュメント	説明
Firepower Compatibility Guide	『Firepower Compatibility Guide』を参照し、Firepower Management Center および Firepower Threat Defense のデバイス アプライアンス モデルのバージョンサポートを確認してください。
Firepower Installation and Configuration Guides	Firepower アプライアンスのインストールと設定の方法については、『Firepower Installation and Configuration Guides』を参照してください。
Firepower Management Center Configuration Guide	『Firepower Management Center Firepower Management Center Configuration Guide』を参照して、Firepower アプライアンスのライセンスと、 Firepower Management Center によって管理される Firepower Threat Defense デバイス 、アクセス コントロール ポリシー、侵入ポリシー、およびファイルポリシーの設定を確認してください。

要件とベストプラクティス

セキュリティ分析とロギング（オンプレミス）を展開してファイアウォールのイベントデータを保存するための要件とベストプラクティスを次に示します。

次の表に、セキュリティ分析とロギング（オンプレミス）の展開でファイアウォールのイベントデータの保存に マネージャ の使用が必要なソリューションのコンポーネントの概要を示します。

ファイアウォール アプライアンス

次のファイアウォール アプライアンスを展開する必要があります。

ソリューションのコンポーネント	必要なバージョン	シスコのセキュリティ分析とロギング（オンプレミス）のライセンス	注記
Firepower Management Center（ハードウェアまたは仮想）	v7.0+ 以前のバージョンを実行している Firepower Management Center の場合は、https://cisco.com/go/sal-on-prem-docsを参照してください。	なし	• Firepower Management Center ごとに 1 つの マネージャ。また、必要に応じて 1 つのフローコレクタと 1 つのデータストア（データノード X 3）を展開できます。
Firepower 管理対象のデバイス FMC によって管理される Firepower Threat Defense デバイス（ハードウェアまたは仮想）	v7.0+（ウィザードを使用） Firepower Threat Defense v6.4 以降（syslog を使用） NGIPS v6.4（syslog を使用）	なし	1 つの Firepower Management Center で管理される複数の Firepower Threat Defense デバイスが同じ Secure Network Analytics 展開にイベントをエクスポートできます。
ASA デバイス	v9.12+	なし	• セキュリティ分析とロギング（オンプレミス） アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。

Secure Network Analytics アプライアンス

Secure Network Analytics の展開には次のオプションがあります。

- 単一ノード：マネージャ のみを展開してイベントを取り込んで保存したり、イベントを確認および照会します。
- マルチノード：フローコレクタを展開してイベントを取り込み、データストアを展開してイベントを保存し、マネージャ を展開してイベントを確認および照会します。

（注） Secure Network Analytics ハードウェアと Secure Network Analytics VE アプライアンスを混在させて展開することはできません。

表 *3*：単一ノード

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
マネージャ	Secure Network Analytics v7.3.1+	なし	• マネージャ 2210 ハードウェアアプライアンスまたはマネージャ の仮想エディション（VE）のいずれかを展開できます。 • 複数台の Firepower Threat Defense デバイスからイベントを受信できます。これらはすべて 1 つの Firepower Management Center によって管理されます。 • イベントを取り込んで マネージャ の Web アプリケーションでファイアウォールイベントを表示するには セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリケーション v2.0+	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。

表 *4:* マルチノード

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス） のライセンス	注記
マネージャ	Secure Network Analytics v7.3.2+	なし	• マネージャ 2210 ハードウェアアプライアンスまたはマネージャ の仮想エディション（VE）のいずれかを展開できます。 • イベントを取り込んで マネージャ の Web アプリケーションでファイアウォールイベントを表示するには セキュリティ分析とロギング（オンプレミス）アプリケーションをインストールする必要があります。

ソリューションのコンポーネント	必要なバージョン	セキュリティ分析とロギング（オンプレミス）のライセンス	注記
Flow Collector	Secure Network Analytics v7.3.2+	なし	• Flow Collector 4210 ハードウェアアプライアンスまたはフローコレクタ VE アプライアンスのいずれかを展開できます。 • 複数台の Firepower Threat Defense デバイスからイベントを受信できます。これらはすべて 1 つの Firepower Management Center によって管理されます。 • 複数の ASA デバイス（v7.4+）から ASA イベントを受信できます。
データストア（データノード X 3）	Secure Network Analytics v7.3.2+	なし	• Data Store 6200（データノード X 3）ハードウェアまたはデータストア VE（データノード VE X 3）のいずれかを展開できます。 • フローコレクタで受信したファイアウォールイベントを保存できます。
セキュリティ分析とロギング（オンプレミス）アプリケーション	セキュリティ分析とロギング（オンプレミス）アプリケーション v2.0+	GB/日に基づくスマートライセンスのロギングおよびトラブルシューティング	マネージャにこのアプリケーションをインストールし、syslog の取り込みを有効にするように設定します。

これらのコンポーネントに加えて、すべてのアプライアンスが NTP を使用して時刻を同期できることを確認する必要があります。

Firepower または Secure Network Analytics アプライアンスのコンソールにリモートでアクセスする場合は、SSH 経由のアクセスを有効にできます。

Secure Network Analytics のライセンス

ライセンスなしで、セキュリティ分析とロギング（オンプレミス） を 90 日間評価モードで使用できます。90 日間経過した後も セキュリティ分析とロギング（オンプレミス） の使用を継続するには、ファイアウォール展開から Secure Network Analytics アプライアンスに syslog データで送信する見込みの 1 日あたりの GB に基づいて、スマートライセンスのロギングとトラブルシューティングのスマートライセンスを取得する必要があります。

（注） ライセンスの計算のために、データ量は最も近い GB 数（切り捨て）で報告されます。たとえば、1 日あたり 4.9 GB を送信する場合は、4 GB と報告されます。

Secure Network Analytics アプライアンスのライセンスに関する詳細については、『Secure Network Analytics Smart Software Licensing Guide』を参照してください。

Secure Network Analytics Resource Allocation

セキュリティ分析とロギング（オンプレミス） に展開した場合、Secure Network Analytics は次の取り込みレートを提供します。

- ハードウェアまたはバーチャルエディション（VE）の 単一ノード の展開では、平均で最大約 20,000 イベント/秒（EPS）でショートバーストでは最大 35,000 EPS を取り込むことができます。
- 3 つのデータノードを備えたバーチャルエディション（VE）マルチノード の展開では、平均で最大約 50k EPS を取り込むことができ、最大 175k EPS の短いバーストが可能です。
- 3 つのデータノードを備えたハードウェア マルチノード の展開では、平均で最大約 10 万 EPS、ショートアーストでは最大 350,000 EPS を取り込むことができます。

割り当てたハードドライブストレージに基づいて、数週間または数か月にわたってデータを保存できます。これらの推定値は、ネットワーク負荷、トラフィックスパイク、イベントごとに送信される情報など、さまざまな要因の影響を受けます。

（注） EPS の取り込みレートが高いと、セキュリティ分析とロギング（オンプレミス） アプリケーションがデータをドロップする場合があります。さらに、接続、侵入、ファイル、マルウェアのイベントのみではなく、すべてのイベントタイプを送信する場合は、全体的な EPS の増加にしたがい、データをドロップする場合があります。この場合はログファイルを確認します。

単一ノード 推奨事項

マネージャ VE リソース

最適なパフォーマンスを得るために、マネージャ VE を展開する場合は、次のリソースを割り当てます。

リソース	推奨
CPU	12
RAM	64 GB
ハードドライブストレージ	2 TB

マネージャ 2210 仕様

ハードウェアの仕様については、マネージャ 2210 仕様書を参照してください。

推定保持期間

マネージャ VE に割り当てるストレージスペースに基づいて、またはマネージャ 2210 を使用している場合は、単一ノード のみの展開でおおよそ次の時間枠のデータを保存できます。

平均 EPS	平均日次イベント	1 TB ストレージの推定保持期間	2TB ストレージの推定保持期間	4 TB ストレージ（ハードウェア）の推定保持期間
1,000	8,650 万	250 日	500 日	1000 日
5,000	4 億 3,000 万	50 日	100 日	200 日
10,000	8 億 6,500 万	25 日	50 日	100 日
20,000	17 億 3,000 万	12.5 日	25 日	50 日

マネージャが最大ストレージキャパシティに達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。

（注） この推定取り込みおよび保管の期間について、これらのリソース割り当てでマネージャ VE をテストしました。仮想アプライアンスに十分な CPU または RAM を割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。ストレージ割り当てを 2 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

マルチノード 推奨事項

最適なパフォーマンスを得るために、マネージャ VE、フローコレクタ VE、およびデータストア VE を展開する場合は、次のリソースを割り当てます。

表 *5*: マネージャ *VE*

リソース	推奨
CPU	8
RAM	64 GB
ハードドライブストレージ	480 GB

表 *6*: *Flow Collector VE*

リソース	推奨
CPU	8
RAM	70 GB
ハードドライブストレージ	480 GB

表 *7*: データノード *VE*（データストアの一部として）

リソース	推奨
CPU	データノードあたり 12
RAM	データノードあたり 32 GB
ハードドライブストレージ	データノード VE あたり 5 TB、または 3 つのデータノードで合計 15 TB

ハードウェア仕様

ハードウェアの仕様については、アプライアンスの仕様書を参照してください。

推定保持期間（3 つのデータノード）

データストア VE に割り当てるストレージスペースに基づいて、またはハードウェア展開がある場合は、マルチノード展開でおおよそ次の時間枠でデータを保存できます。

平均 EPS	平均日次イベント	仮想	ハードウェア
1,000	8,650 万	1,500 日	3,000 日
5,000	4 億 3,000 万	300 日	600 日
10,000	8 億 6,500 万	150 日	300 日
20,000	17 億 3,000 万	75 日	150 日
25,000	21 億 6,000 万	60 日	120 日
50,000	43 億 2,000 万	30日間	60 日
75,000	64 億 8,000 万	サポート対象外	40 日間
100,000	86 億 4,000 万	サポート対象外	30日間

データストアが最大ストレージキャパシティに達すると、着信データ用のスペースを確保するために最も古いデータが最初に削除されます。

（注） この推定取り込みおよび保存の期間について、これらのリソース割り当てでこれらの仮想アプライアンスをテストしました。仮想アプライアンスに十分なCPUまたはRAMを割り当てないと、リソース割り当てが不十分なために予期しないエラーが発生する場合があります。データノードのストレージ割り当てを 5 TB を超えて増やすと、リソース割り当てが不十分なために予期しないエラーが発生する可能性があります。

通信ポート

次の表に単一ノードの展開の場合にセキュリティ分析とロギング（オンプレミス）を統合するために開く必要がある通信ポートを示します。

表 *8*：単一ノード

送信元（クライアント）	宛先（サーバ）	ポート	プロトコルまたは目的
FMC、FTDデバイス、およびマネージャ	外部インターネット（NTP サーバー）	123/UDP	すべて同じ NTP サーバへの NTP 時刻同期

送信元（クライアント）	宛先（サーバ）	ポート	プロトコルまたは目的
ユーザーワークステーション	FMCおよびマネージャ	443/TCP	Webブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン
FMC によって管理される FTD デバイス	マネージャ	8514/UDP	Firepower Threat Defense デバイスからの syslog のエクスポート、マネージャ への取り込み
FMC	マネージャ	443/TCP	FMC から マネージャ へのリモートクエリ

次の表に マルチノード の展開の場合に セキュリティ分析とロギング（オンプレミス） を統合するために開く必要がある通信ポートを示します。さらに、Secure Network Analytics 展開のために開く必要があるポートについては、「x2xx シリーズ ハードウェアアプライアンス設置ガイド」または「Virtual Edition アプライアンス インストール ガイド」を参照してください。

表 *9:* マルチノード

送信元（クライアント）	宛先（サーバ）	ポート	プロトコルまたは目的
FMC、FTDデバイス、マネージャ、フローコレクタ、およびデータストア	外部インターネット（NTP サーバー）	123/UDP	すべて同じ NTP サーバへの NTP 時刻同期
ユーザワークステーション	FMCおよびマネージャ	443/TCP	Webブラウザを使用した HTTPS 経由でのアプライアンスの Web インターフェイスへのログイン
FMC によって管理される FTD デバイス	Flow Collector	8514/UDP	FTD デバイスからの syslog のエクスポート、フローコレクタへの取り込み
ASA デバイス	Flow Collector	8514/UDP	ASA デバイスからの syslog のエクスポート、フローコレクタへの取り込み

送信元（クライアント）	宛先（サーバ）	ポート	プロトコルまたは目的
FMC	マネージャ	443/TCP	FMC から マネージャへのリモートクエリ

設定の概要

次に、イベントデータを保存するための展開の大まかな設定手順を説明します。

導入を開始する前に、次のタスクを確認してください。

コンポーネントとタスク	手順
単一ノード の導入	次の選択肢があります。 • マネージャ 2210 をネットワークに展開し、eth0 管理インターフェイスの IP アドレスやその他の情報の割り当てを含む初期設定を実行します。詳細については、『x2xx Series Hardware Installation Guide』と『Secure Network Analytics System Configuration Guide』を参照してください。 • マネージャ VE ISO をダウンロードし、マネージャ VE をハイパーバイザに展開します。初期設定を実行し、eth0 管理インターフェイスの IP アドレスとその他の情報を割り当てます。詳細については、『Secure Network Analytics Virtual Edition Installation Guide』を参照してください。
マルチノード の導入	次の選択肢があります。 • ハードウェア マネージャ、フローコレクタ、および 3 つのデータノードをネットワークに展開します。各アプライアンスの初期設定を実行し、データストアを初期化します。詳細については、『x2xx Series Hardware (with Data Store) Appliance Installation Guide』を参照してください。 • マネージャ VE ISO、フローコレクタ VE ISO、およびデータノード ISO をダウンロードします。1 つの マネージャ VE、1 つのフローコレクタ VE、および 3 つのデータノード VE をハイパーバイザに展開します。各アプライアンスの初期設定を実行し、データストアを初期化します。詳細については、『Virtual Edition (with Data Store) Appliance Installation Guide』を参照してください。

コンポーネントとタスク	手順
セキュリティ分析とロギング（オンプレミス） アプリケーションをダウンロードして マネージャにインストールし、ファイアウォールのイベントを受信して保存するように Secure Network Analytics の展開を設定	• マネージャ で、[集中管理（Central Management）] の [アプリケーションマネージャ（App Manager）] に移動し、 アプリケーションをダウンロードします。Firepower デバイスからイベントを受信するように設定します。 • アプリケーションの使用方法の詳細については、セキュリティ分析とロギング（オンプレミス）リリースノートとアプリケーションのヘルプを参照してください。
イベントを セキュリティ分析とロギング（オンプレミス）に送信するように Firepower Management Center を設定	次の選択肢があります。 • イベントを Secure Network Analytics アプライアンスに送信するように Firepower Management Center を設定します。 • 「Configure Data Plane Event Logs」を使用して、データ プレーン イベント ロギングを設定します。 • 「Stop Storing Low-Priority Connection Events on the Firepower Management Center」を使用して、Firepower Management Center のロギング負荷を軽減します。
イベントを セキュリティ分析とロギング（オンプレミス）に送信するように ASA デバイスを設定	• イベントを Secure Network Analytics アプライアンスに送信するように ASA デバイスを設定します。「ASA Devices Configuration」を参照してください。 • ASA イベントは、セキュリティ分析とロギング（オンプレミス）アプリケーション v3.0.0+ および Secure Network Analytics v7.4.0+ マルチノード展開でサポートされています。
次の手順の確認	次の手順を確認します。 • 詳細については、Firepower のオンラインヘルプを参照してください。「Work in Firepower Management Center with Connection Events Stored on a Secure Network Analytics」を参照してください。 • Secure Network Analytics の使用方法については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。

次のステップ

セキュリティ分析とロギング（オンプレミス） の一部として syslog イベントデータを Secure Network Analytics アプライアンスに渡すようにファイアウォール展開を設定したら、次の手順を実行できます。

- FMC オンラインヘルプを確認します。
- Secure Network Analytics の詳細については、マネージャ Web アプリケーションのオンラインヘルプを参照してください。

次のステップ

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。